

**REMARKS**

Applicant thanks the examiner for accepting the drawings filed on December 19, 2005.

Applicant also thanks the examiner for acknowledging Applicant's claim for priority under 35 U.S.C. § 119 and acknowledging receipt of certified copy of the priority document filed in this National Stage application.

Claims 1-20 have been presented for examination. Applicant thanks the Examiner for indicating that these claims are allowable and would be allowed once objections to the preamble of the independent claims 1, 4, 7, 8, 11, 12, 19 and 20 have been overcome.

The preamble to these claims has been amended to make it clearer that the invention involves applying a padding scheme that is conventionally used in cryptosystems not using random numbers, to cryptosystems in which a random number is used to create cybertext, the random number being susceptible to recovery at a receiving end.

In the Background portion of the subject application, for example, at page 8, it is noted that certain padding schemes are applied to cryptosystems that do not use random numbers. While ensuring security in such systems not using random numbers, those padding schemes do not ensure security in cryptosystems that use random numbers. As explained, for example, at page 10 of the subject application, the importance of the invention of the subject application is that it has found a way to apply a padding scheme to cryptosystems in which the receiver of a ciphertext can recover a random number as well as plain text, thus ensuring security. That is, according to the teachings of the subject invention, Applicant has discovered a way of applying a

RESPONSE TO QUAYLE ACTION  
U.S. Appln. No. 10/561,216  
Attorney Docket No.: Q92077

padding scheme previously proposed for cryptosystems that do not use a random number to cryptosystems that use a random number that can be recovered at a receiver to assure security.

In view of the foregoing, it is respectfully submitted that the objections to the claims have been overcome and that this application is now in condition for allowance.

For any reason that the examiner find the application other than in condition for allowance it is respectfully requested to call the undersign attorney at the Washington, DC telephone no. (202) 293-7060 to discuss the steps necessary for placing the application in condition for allowance.

SUGHRUE MION, PLLC  
Telephone: (202) 293-7060  
Facsimile: (202) 293-7860

WASHINGTON OFFICE

**23373**

CUSTOMER NUMBER

Respectfully submitted,  
/Howard L. Bernstein/hlb  
Howard L. Bernstein  
Registration No. 25,665

Date: June 18, 2007